Cyber Security Policy

POLICY TITLE: Cyber Security Policy

POLICY CATEGORY: COLLEGE ADMINISTRATIVE

POLICY NUMBER:

POLICY VERSION: 1

POLICY OWNER: VP Digital Transformation and Chief Information Officer

APPROVAL DATE: Click or tap to enter a date.

EFFECTIVE DATE: Click or tap to enter a date.

POLICY APPROVER: Board of Governors

REVIEW PERIOD: Every 5 Years (or as needed)

REVIEWED: 6/24/2024

REVISED: N/A Click or tap to enter a date.

1. Purpose

This policy aims to establish the strategy and direction for protecting George Brown College (GBC) Technology Assets and to provide directives on how GBC will safeguard its confidentiality, integrity, and availability.

Ethical considerations have been integrated into GBC's Cyber Security strategy, tools, and controls, primarily emphasizing digital inclusivity, accessibility, and equity. All GBC users shall have equitable access and benefit from GBC's secured digital technologies. GBC is committed to continually assessing its Cyber Security practices to ensure adherence to best practices while also considering the voices of our diverse community of students, employees, and other stakeholders. This policy, along with the related policies and standards outlined below, was established to foster trust and inclusion in the digital domain and ensure:

a) **Protection of Information**: Protect GBC information from unauthorized access, modification, or destruction.
b) **Regulatory Compliance**: Comply with legal and regulatory information security and privacy requirements.
c) **Risk Management**: Manage risks associated with cyber threats and vulnerabilities.
d) **Education and Awareness**: Foster an influential Cyber Security culture.
e) **Incident Response**: Have a clear and well-defined process for detecting and responding to Cyber Security incidents.
f) **System Integrity**: Ensure the integrity, availability, and reliability of the college's information and Information Systems.
g) **Continual Improvement**: Continuously improve the college's Cyber Security controls and processes based on regular consultations, audits, reviews, and self-assessments.
h) **Digital Inclusivity, Accessibility, and Equity:** Provide equitable access **a**nd benefit from digital technologies and online resources for all GBC Users**.**

2. Scope

This policy applies to all GBC Users, including but not limited to students, employees, consultants, contractors, sub-contractors, vendors, temporary workers, guests, trusted partners, alums, board members, and agents of the GBC. This policy shall be read with the policies and standards outlined in the Related Materials and Related Policies section.

3. Definition of Terms

Please see this link for all Cyber Security definitions.

4. Policy

4.1 Roles and Responsibilities

4.1.1 Operational Management

a) **All Users shall be responsible for the following:**

- **Policy Compliance:** Understand and conduct their activities per the established Cyber Security Policy and associated standards, maintaining a commitment to protecting GBC's Technology Assets and data.

- **Mandatory Training:** All employees must complete the assigned Cyber Security awareness training. This will equip employees with the knowledge and skills to identify, prevent, and report potential security incidents.
- **Incident Reporting:** Any suspicion or discovery of potential Cyber Security incidents involving GBC Technology Assets shall be promptly reported to respective managers, Cyber Security, or the Information Technology Services Division.
- **Information Protection:** Safeguard information they have access to, ensuring it is protected according to its sensitivity and criticality. This includes adhering to the best information creation, storage, use, transmission, archival, and disposal practices.
- **Continuous Vigilance:** Maintain a vigilant mindset, stay updated on new threats, and follow the evolving Cyber Security guidelines issued by the college.

4.1.2 Risk Management, Audit, and Compliance

a) **The Cyber Security department shall be responsible for the following:**

- **Governance Oversight:** Supervise the governance of Cyber Security, ensuring a clear, strategic direction that aligns with the college's mission, vision, and objectives.
- **Policy Development and Monitoring:** Develop and enhance Cyber Security standards, procedures, and controls while ensuring compliance. Review and update these policies regularly to keep pace with evolving threats.
- **Risk Minimization Strategies:** Devise strategies to deter potential misuse, damage, and unauthorized use of information, thereby fortifying overall security.
- **Cyber Security Awareness:** Ensure widespread understanding of Cyber Security risks across the college, promoting a culture of Cyber Security.
- **Consultation and Advice:** Gather feedback and provide consultation services, providing timely and effective risk mitigation strategies.
- **Program Benchmarking:** Conduct regular reviews of the Cyber Security program, benchmark it against industry standards, and report findings/gaps.
- **Audits:** Undertake comprehensive assessments and audits, objectively evaluating the adequacy and effectiveness of Cyber Security controls. This audit process ensures the integrity of GBC's Cyber Security measures, identifies areas for improvement, and ensures equitable practices are maintained.

4.1.3 Enterprise Risk Management shall be responsible for the following:

- **Cyber Security Risk Integration**: Cyber Security risks are integrated and intrinsic to the overarching Enterprise Risk Management (ERM) framework.

4.1.4 Information and Technology Governance shall be responsible for the following:

- **Decision-making and coordination:** Play a vital role in fostering communication and coordination across GBC for technology. The committee (or its sub-committee) is responsible for disseminating pertinent information, reviewing and setting Cyber Security priorities, and assessing potential

security impacts to ensure a coordinated and robust response to evolving Cyber Security challenges.

4.2 Cyber Security Principles

The protection of GBC Technology Assets is vital to the academic and administrative functions of the college. The following principles aim to safeguard the college's digital infrastructure from potential cyber threats and ensure safety. They promote a culture of cyber awareness and responsibility, reflecting our commitment to providing a secure and resilient digital environment.

4.2.1 Information and Technology Governance: Accountability and responsibility for Cyber Security are integral to GBC's mission. GBC will consistently employ best practices, ensuring Users adhere to relevant Cyber Security policies, standards, procedures, and practices in all activities.

4.2.2 Information Protection: GBC is responsible for protecting personal information in its possession, per Ontario's Freedom of Information and Protection of Privacy Act (FIPPA). GBC shall consistently strive to meet high standards, ensuring strong information protection and respect for individuals' rights.

4.2.3 Transparency & Accountability: GBC users shall be provided with the required information to understand how their data is collected, stored, processed, and protected at GBC.

4.2.4 Continuous Awareness and Training: GBC will endeavor to host a continuous Cyber Security awareness and training program. This program is designed to foster a culture of mindfulness of security, informing Users about emerging threats and their responsibilities to secure GBC Technology Assets.

4.2.5 Asset Security: GBC Technology Assets have value and shall be inventoried, protected, and secured to a level appropriate to their sensitivity, criticality, and the college's risk tolerance. GBC Technology Assets shall be protected from unauthorized access, modification, destruction, or disclosure. Technology Asset Owners, typically department leaders and managers, will ensure adequate safeguards are in place to mitigate any risks to the information contained within these Technology Assets.

4.2.6 Identity and Access Management: GBC Technology Asset Owners are accountable for overseeing access rights, roles, and privileges, emphasizing least privilege and segregation of duties. Access to GBC Systems is granted based on individual role-based needs and managerial approval.

4.2.7 Cyber Security Risk Management: Cyber Security risk assessments are conducted for new and existing GBC Information and Information Systems to keep abreast with the evolving requirements and align with regulatory, contractual, and business requirements, ensuring a proactive and agile response to risk management.

4.2.8 Operations Management: Backup and restoration procedures are in place, emphasizing support for on-premises and cloud solutions. Development, testing, and production activities shall be performed in separate environments to reduce the risk of unauthorized access or changes while processes are in place to ensure appropriate segregation of duties for critical operations or activities.

4.2.9 Communications Security: Controls are implemented to protect information in networks and their supporting information processing facilities, ensuring the security and integrity of data during transmission.

4.2.10 Logging and Monitoring: Information Systems activities are logged and monitored to detect policy violations and anomalous/malicious behavior. Audit logs, records, and reports are protected from unauthorized access, modification, misuse, or compromise. Cyber Security conducts periodic reviews and security assessments of Information Systems.

4.2.11 Cyber Security Incident Management: Cyber Security maintains comprehensive logs and monitors access to IT systems to prevent and detect Cyber Security breaches. Upon detecting potential or actual Cyber Security incidents, GBC Cyber Security is immediately alerted, followed by an incident management and response process.

4.2.12 Third-Party Service/Risk Management: Due diligence is exercised when selecting Third-Party Service Providers (TSPs). TSPs are contractually and legally required to comply with GBC's Cyber Security requirements and enter confidentiality/non-disclosure agreements. TSPs shall be assessed to ensure their Cyber Security posture aligns with GBC's Cyber Security requirements and risk appetite before entering contractual relationships with GBC. All third-party connectivity to the GBC network requires Cyber Security approval and oversight.

Each TSP has an accountable GBC Technology Asset Owner who regularly reviews access or provisioning provided. The Technology Asset Owner ensures that the Cyber Security controls, service definition, and delivery levels in the third-party agreements are implemented and that services are maintained during transition periods.

4.2.13 Acquisition, Development, and Maintenance: New IT solutions shall integrate Cyber Security requirements and involvement from inception. Technology and Cyber Security changes shall be controlled as per the appropriate change management practices, ensuring the integrity and security of the systems.

4.2.14 Cyber Security Aspects of Business Continuity Management: The requirements for the continuity of Cyber Security operations in adverse situations (e.g., during a crisis or disaster) will be documented in GBC's Cyber Incident Response plan. In conjunction with ITS's Disaster Recovery and GBC's Business Continuity plans, this plan shall be regularly tested and updated to remain current and effective.

4.2.15 Security and Privacy by Design: This principle is integral to our approach in developing and implementing secure systems and solutions throughout all phases of their lifecycle to implement effective risk management strategies. By embedding Cyber Security and privacy requirements early, GBC strives to minimize vulnerabilities and maintain a resilient and adaptable digital environment committed to protecting our sensitive data while ensuring that security and data privacy are integrated into all systems, software, and solutions.

4.2.16 Continuous Improvement: Cyber Security ensures the ongoing enhancement of the GBC's Cyber Security program by consistently measuring and monitoring its effectiveness and efficiency, making changes as necessary, and advocating for constant improvement.

4.2.17 Accessibility and Equity: GBC is responsible for providing all users equitable access to and benefits from digital technologies and online resources.

5. Compliance

This policy serves as the guiding document for all GBC Users. Users are expected to adhere to this policy and seek clarification on ambiguous aspects. Non-compliance with any aspects of this policy and its related standards may result in consequences aligned with the severity of the infraction and in alignment with any applicable collective agreements or Student Code of Conduct. Any non-compliance/policy violation should be reported to cybersecurity@georgebrown.ca.

Students:

- Students shall be aware of this policy and redirect any questions about it or its provisions to the Cyber Security team.
- Repercussions for students can range from a warning to more severe measures, such as the temporary or permanent suspension of digital access privileges or accounts. Any academic sanctions will align with the related Student Code of Conduct.

Faculty/Employees:

- Department leaders and their employees shall be aware of this policy and redirect any questions about it or its provisions to the Cyber Security team.
- Repercussions for staff can include revocation of access privileges, disciplinary actions, or termination of employment or contract. Repercussions will be in alignment with applicable collective agreements.

Contractors/3rd Parties:

- Contract owners are responsible for ensuring that any third parties (vendors, suppliers) providing services and solutions to the college understand and adhere to this policy.
- In the event of non-compliance or policy breaches by third parties, appropriate actions will be undertaken per contractual/legal agreements.

6. Exceptions

While adherence to this policy is mandatory for all GBC Users, under exceptional circumstances where compliance may not be feasible or could impede legitimate operational requirements, an exception shall be granted by the VP, Digital Transformation & CIO. The approval will be time-bound and not regarded as an indefinite waiver.

Related Materials

This policy is aligned with the ISO 27000 family of standards (Information Security Management System (ISMS)).

ISO Standards:

- ISO 27001: 2022 - Information Technology - Security Techniques - Information Security Management System (ISMS): Requirements

- ISO 27002: 2022 - Information Technology - Security Techniques - Code of practice for Information Security controls
- ISO 27005: 2022 Information security, Cyber Security and privacy protection — Guidance on managing information security risks

Regulations:

- Government of Canada. (2019). Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5).

Related Policies

Acceptable Use Policy	**Clear Desk and Clear Screen Standard**	**Employee Code of Conduct – Academic**	**Employee Code of Conduct - Admin**
Employee Code of Conduct - Staff	**Multi-Factor Authentication Policy**	**Privacy Policy**	